IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

Stephen J. Vash, individually and on behalf of all others similarly situated, Plaintiff, vs. T-Mobile US, Inc., Defendant.	CASE NO. **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Stephen J. Vash ("Vash" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant T-Mobile US, Inc. ("T-Mobile" or "Defendant") based on his personal knowledge and the investigation of counsel and alleges as follows:

INTRODUCTION

1. This is a class action brought by Plaintiff on behalf of himself and the more than one hundred million (100,000,000) other similarly situated persons whose personal information was acquired and/or accessed by unauthorized persons in the data breach that T-Mobile announced on August 16, 2021 (the "Data Breach").

2. T-Mobile provides wireless voice, messaging, and data services in the United States, Puerto Rico and the U.S. Virgin Islands under the T-Mobile and Metro by T-Mobile brands. The company operates the second largest wireless network in the U.S. market with over 100 million customers and annual revenues of more than

$68 billion.

3. Plaintiff and other members of the proposed class were required, as current or prospective customers of T-Mobile, to provide T-Mobile with sensitive personal information to apply for and/or receive wireless voice, messaging, and data services. T-Mobile assured Plaintiff and other members of the proposed class that their personal information would be kept safe from unauthorized access. The T-Mobile Privacy Policy touts as follows: "We use administrative, technical, contractual, and physical safeguard designed to protect your data while it is under our control."

4. T-Mobile betrayed the trust of Plaintiff and other members of the proposed class by failing to properly safeguard and protect their sensitive personal information, enabling cybercriminals to acquire and/or access it.

5. Plaintiff brings this class action against T-Mobile for its failure to properly secure and safeguard the personally identifiable information of Plaintiff and other members of the proposed class stored within T-Mobile's information network, including, without limitation, first and last names, dates of birth, social security numbers, driver's license/ID information, physical addresses, phone numbers, unique International Mobile Equipment Identity (or "IMEI") numbers, and/or account PINs (these types of information, *inter alia*, being hereafter referred to,

collectively, as "personally identifiable information" or "PII").[1]

6. T-Mobile disregarded the rights of Plaintiff and other members of the proposed class by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and other members of the proposed class was safeguarded. Specifically, T-Mobile ignored the rights of Plaintiff and other members of the proposed class by, inter alia, intentionally, willfully, recklessly or negligently failing to (1) ensure the security and confidentiality of consumer records and PII; (2) protect against anticipated threats or hazards to the security or integrity of consumer records and PII; (3) protect against unauthorized access to or use of consumer records or PII that could result in substantial harm or inconvenience to any current or prospective customer; (4) implement or maintain policies and procedures that adequately secured consumers' records and PII; (5) sufficiently monitor, audit and update its cybersecurity procedures and patch maintenance; and (6) timely detect the Data Breach, mitigate harm, and notify consumers of the Data Breach. As a result, the PII of Plaintiff and

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

other members of the proposed class was compromised through disclosure to and access by one or more unknown and unauthorized third parties.

7. Plaintiff and other members of the proposed class have suffered injury because of T-Mobile's conduct. These injuries include: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (g) the diminished value of Plaintiff's and Class members' PII; (h) the diminished value of T-Mobile's services Plaintiff and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiff's and Class members' PII on the dark web.

8. In addition to remedying the harms suffered because of the Data

Breach, Plaintiff and the other 100+ million consumers similarly situated also have a significant interest in preventing additional data breaches because their PII remains in T-Mobile's possession without adequate protection.

9. Representative Plaintiff brings this action on behalf of all persons whose PII was compromised because of T-Mobile's failure to: (i) adequately protect the PII of Plaintiff and other members of the proposed class; (ii) warn Plaintiff and other members of the proposed class of these inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. T-Mobile's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff seeks actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to T-Mobile's data security systems and protocols (which have been the subject of multiple recent data breaches), future annual audits, T-Mobile-funded long-term credit monitoring services, and any other remedies the Court deems necessary and proper.

THE PARTIES

11. Plaintiff is a citizen and resident of the State of Georgia and was a Georgia resident during the period when the data breach occurred.

12. Plaintiff is and has been a customer of, and received wireless voice,

messaging, and data services from, T-Mobile. The reports regarding the breadth and severity of the Data Breach and T-Mobile's disclosures concerning the number and class of consumers affected indicate, upon information and belief, that Plaintiff and Plaintiff's data have been impacted.

13. To receive wireless voice, messaging, and data services from T-Mobile, Plaintiff was required to provide T-Mobile with sensitive PII. Plaintiff's PII was within the possession and control of T-Mobile at the time of the Data Breach.

14. Plaintiff brings this action on behalf of himself, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

15. Defendant T-Mobile US, Inc. is a Delaware corporation with its principal place of business located at 12920 SE 38th Street, Bellevue, Washington 98006. T-Mobile has a corporate office located at 1 Ravinia Dr. NE, Atlanta, Georgia 30346.

16. T-Mobile provides wireless voice, messaging, and data services in the United States, Puerto Rico, and the U.S. Virgin Islands under the T-Mobile and Metro by T-Mobile brands. The company operates the second largest wireless network in the U.S. market with over 100 million customers.

17. T-Mobile has access to enormous resources. In 2020, T-Mobile

reported total revenues of more than $68 billion and net income of more than $3 billion. In that same fiscal year, T-Mobile reported total assets of more than $200 billion.

JURISDICTION AND VENUE

18. This Court has diversity jurisdiction over this action pursuant to 28 U.S.C. §1332 because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and upon information and belief, at least one other member of the proposed class is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because Defendant has a corporate office in the State of Georgia, routinely conducts business in Georgia, has sufficient minimum contacts in Georgia, and has intentionally availed itself of this jurisdiction by marketing and selling products and services in Georgia.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant has a corporate office located in the District, Defendant conducts a substantial amount of its business in this District, and the events that give rise to Plaintiff's claims occurred in part in this District.

FACTUAL ALLEGATIONS

The Breach

21. On August 15, 2021, it was first reported by Vice.com that the T-Mobile computer systems had been hacked. At some point prior to August 15, 2021, a cybercriminal had acquired and was actively selling data related to over 100 million people from the T-Mobile servers and the data included sensitive PII. The cybercriminal told Vice.com that it appeared T-Mobile was aware of the breach because he or she lost access to the backdoored servers that had been breached and accessed.

22. T-Mobile acknowledged the breach on August 16, 2021, stating in a press release that it "determined that unauthorized access to some T-Mobile data occurred."

23. On August 17, 2021, T-Mobile issued the following press release:

> As we shared yesterday, we have been urgently investigating the highly sophisticated cyberattack against T-Mobile systems, and in an effort to keep our customers and other stakeholders informed we are providing the latest information we have on this event and some additional details:
>
> - Late last week we were informed of claims made in an online forum that a bad actor had compromised T-Mobile systems. We immediately began an exhaustive investigation into these claims and brought in world-leading cybersecurity experts to help with our assessment.
> - We then located and immediately closed the access point that we believe was used to illegally gain entry to our servers.

- Yesterday, we were able to verify that a subset of T-Mobile data had been accessed by unauthorized individuals. We also began coordination with law enforcement as our forensic investigation continued.
- While our investigation is still underway and we continue to learn additional details, we have now been able to confirm that the data stolen from our systems did include some personal information.
- We have no indication that the data contained in the stolen files included any customer financial information, credit card information, debit or other payment information.
- Some of the data accessed did include customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of current and former postpay customers and prospective T-Mobile customers.
- Our preliminary analysis is that approximately 7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile. Importantly, no phone numbers, account numbers, PINs, passwords, or financial information were compromised in any of these files of customers or prospective customers.
- As a result of this finding, we are taking immediate steps to help protect all of the individuals who may be at risk from this cyberattack. Communications will be issued shortly to customers outlining that T-Mobile is:

    - Immediately offering 2 years of free identity protection services with McAfee's ID Theft Protection Service.
    - Recommending all T-Mobile postpaid customers proactively change their PIN by going online into their T-Mobile account or calling our Customer Care team by dialing 611 on your phone. This precaution is despite the fact that we have no knowledge that any postpaid account PINs were compromised.
    - Offering an extra step to protect your mobile account with our Account Takeover Protection capabilities for postpaid customers, which makes it harder for customer accounts to be fraudulently ported out and stolen.

- Publishing a unique web page later on Wednesday for one stop information and solutions to help customers take steps to further protect themselves.
  - Edited to add on 8/18: https://www.t-mobile.com/brand/data-breach-2021

- At this time, we have also been able to confirm approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were also exposed. We have already proactively reset ALL of the PINs on these accounts to help protect these customers, and we will be notifying accordingly right away. No Metro by T-Mobile, former Sprint prepaid, or Boost customers had their names or PINs exposed.
- We have also confirmed that there was some additional information from inactive prepaid accounts accessed through prepaid billing files. No customer financial information, credit card information, debit or other payment information or SSN was in this inactive file.

We take our customers' protection very seriously and we will continue to work around the clock on this forensic investigation to ensure we are taking care of our customers in light of this malicious attack. While our investigation is ongoing, we wanted to share these initial findings even as we may learn additional facts through our investigation that cause the details above to change or evolve.

Plaintiff's Dealings with T-Mobile

24. Plaintiff is and has been a T-Mobile customer for many years, who provided personally identifiable information to T-Mobile in order to maintain postpay mobile services from T-Mobile.

T-Mobile Understood the Value of PII

25. T-Mobile's Privacy Policy states as follows: "We use administrative, technical, contractual, and physical safeguard designed to protect your data while it

is under our control."

26. Notwithstanding these promises, it appears a lone hacker was able to breach T-Mobile's servers and acquire the sensitive PII of more than 100 million current, former, and prospective customers of T-Mobile. There is, therefore, little question that T-Mobile did not to live up to its promises regarding data protection.

27. Server patch management is a routine part of cybersecurity systems, processes, and protection particularly when a company holds consumer PII. However, upon information and belief, T-Mobile learned of the massive breach not through its own proactive and protective cybersecurity systems, but rather were alerted when the hacker revealed the breach on an online chat forum. The fact that T-Mobile purports to have quickly located and closed the access point to the T-Mobile servers suggests that proper maintenance would have ameliorated the threat, that T-Mobile's cybersecurity surveillance systems were lacking and subpar, and that T-Mobile was negligent in maintaining its systems and safeguarding Plaintiff's and Class members' PII.

28. T-Mobile has been the subject of multiple data breaches in recent years and should have been on high alert, particularly with regard to simple routine cybersecurity maintenance.

29. Consumers have many choices for wireless voice, messaging, and data services and they would not have chosen to provide their PII to T-Mobile had they

known that the information would be at heightened risk of compromise due to T-Mobile's lax data security.

Plaintiff and Class Members Have Suffered Harm

30. As a result of the Data Breach, Plaintiff and Class members were deprived of the value in and security of their PII and now face an increased risk of theft, identity theft, fraud, and abuse, and the constant fear, anxiety, and hardship that comes with it. And those impacted by T-Mobile's failure to protect Plaintiff's and Class members' PII will be at risk for identity theft and fraud for years to come.

31. As a result of T-Mobile's unfair, inadequate, and unreasonable data security, at least one cyber-criminal and unknown others now possess the PII of Plaintiff and Class members. With first and last names, date of birth, social security number, and driver's license/ID information (among other information), criminals can open entirely new credit accounts and bank accounts, and garner untold amounts through fraud that victims will not be able to detect until it is too late. Victims' credit profiles can be destroyed, and they will lose the ability to legitimately borrow money, obtain credit, or even open bank accounts.

32. Further, criminals can file false federal and state tax returns in victim's names, preventing or at least delaying victims' receipt of their legitimate tax refunds and potentially making victims targets of IRS and state tax investigations. At the very least, victims must add themselves to credit fraud watch lists, which

substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, or buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home, without taking the time to request that the freeze be suspended, waiting the days it can take for that to occur, and then reinstating the freeze. Further, there are four major reporting agencies, so consumers may need to take these steps with all of them because they will not know which bureau a creditor may consult. Also, in many states, and in many circumstances, such freezes cost the consumer money.

33. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post sensitive personal information for sale.

34. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, SSNs, and other PII directly on various Internet websites and on the dark web making the information publicly available and available to criminals. Moreover, the suspected hacker in this matter has already attempted to sell the PII he/she accessed from the T-Mobile servers on the dark web.

35. The sensitive personal information that T-Mobile failed to adequately protect is "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, and file false federal and state tax returns.

36. Although T-Mobile is offering free credit monitoring to some customers, the credit monitoring services do little to prevent wholesale identity theft. Moreover, experts warn that batches of stolen information will not be immediately dumped on the black market. "[O]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed. . . . They often wait until consumers are less likely to be on the lookout for fraudulent activities." In light of the seriousness of this breach and the nature of the data involved, short-term credit monitoring is decidedly not enough.

37. A cybercriminal, especially one with millions of records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, resulting in thousands of dollars in losses and lost time and productivity. Thus, Plaintiff and Class members must take additional steps to protect their identities. And Plaintiff and Class members must bear the burden and expense of identity and credit monitoring, and heightened vigilance for years to come.

CLASS ACTION ALLEGATIONS

38. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of himself and the following class (collectively, the "Class"):

> All persons residing in the United States whose personal information was acquired or accessed by unauthorized individuals as a result of the breach of T-Mobile US, Inc.'s information system(s) that was announced by T-Mobile US, Inc. on August 16, 2021.

39. The following individuals and entities are excluded from the proposed Class: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

40. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

41. **Numerosity**: The proposed Class is believed to be so numerous that joinder of all members is impracticable. Upon information and belief, the total number of Class members is in the millions of individuals. Membership in the classes will be determined by analysis of Defendant's records.

42. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their PII compromised in the same way by the same conduct of Defendant.

43. **Adequacy**: Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class that he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

44. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation

increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

45. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and Class members' PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether they breached this duty;

d. Whether Defendant's systems, networks, and data security practices used to protect Plaintiff's and Class members' PII violated the FTC Act, and/or Defendant's other duties discussed herein;

e. Whether Defendant knew or should have known that their computer and network security systems were vulnerable to a data breach;

f. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class members and the public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

46. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes in their entireties, not on facts or law applicable only to the Plaintiff.

47. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

CLAIMS FOR RELIEF

First Claim - Negligence

48. Plaintiff incorporates by reference the allegations in paragraphs 11-47 above as though fully set forth herein.

49. At all times herein relevant, Defendant owed Plaintiff and Class members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard the PII of Plaintiff and Class members and to use commercially reasonable

methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and Class members in its computer systems and on its networks.

50. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, and protecting PII in its possession;

b. to protect Plaintiff's and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

c. to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication, including patch maintenance;

d. to adequately monitor, audit, and update the security of its networks and systems including patch maintenance;

e. to implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

f. to recognize in a timely manner that Plaintiff's and other Class members' PII had been compromised;

g. to promptly notify Plaintiff and Class members of any data

breach, security incident, or intrusion that affected or may have affected their PII;

h. to timely detect and mitigate the Data Breach.

51. Defendant knew that the PII of Plaintiff and Class members was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

52. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

53. Defendant knew, or should have known, that cyber criminals routinely target large corporations through cyberattacks to steal sensitive personal information.

54. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' PII.

55. Because Defendant knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the PII contained thereon.

56. Defendant also had independent duties under state and federal laws that

required Defendant to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiff and Class members.

57. Plaintiff's and Class members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII its stored on them from attack.

58. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and Class members.

59. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class members.

60. Defendant breached its general duty of care to Plaintiff and Class members in, but not necessarily limited to, the following ways:

a. failing to exercise reasonable care in obtaining, retaining, securing, and protecting PII in its possession;

b. failing to protect Plaintiff's and Class members' PII in its possession by using reasonable and adequate security procedures and

systems;

c. failing to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication

d. failing to adequately train its employees to not store PII longer than absolutely necessary;

e. failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class members' PII;

f. failing to implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

g. failing to promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

61. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

62. Defendant breached its duty to notify Plaintiff and Class members of

the unauthorized access by failing to notify Plaintiff and Class members immediately after learning of the Data Breach and then by failing to provide Plaintiff and Class members sufficient information regarding the breach.

63. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their PII.

64. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class members and the harm suffered or risk of imminent harm suffered by Plaintiff and Class members. Plaintiff's and Class members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

65. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred because of Defendant's failure to observe these duties, including the loss of privacy, significant risk of identity theft, and Plaintiff's overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

66. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and Class members to provide fair and adequate computer systems and data

security to safeguard the PII of Plaintiff and Class members.

67. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

68. Defendant gathered and stored the PII of Plaintiff and Class members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

69. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and Class members and by not complying with applicable industry standards, as described herein.

70. Defendant breached its duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' PII, and by failing to provide prompt notice without reasonable delay.

71. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

72. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

73. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against.

74. Defendant breached its duties to Plaintiff and Class members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

75. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (g) the diminished value of

Plaintiff's and Class members' PII; (h) the diminished value of T-Mobile's services Plaintiff and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiff's and Class members' PII on the dark web.

76. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Second Claim – Invasion of Privacy

77. Plaintiff incorporates by reference the allegations in paragraphs 11-47 above as though fully set forth herein.

78. Plaintiff and Class members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

79. Defendant owed a duty to Plaintiff and Class members to keep their PII confidential.

80. Defendant allowed unauthorized and unknown third parties access to and acquire the PII of Plaintiff and Class members because it failed to protect the PII.

81. The unauthorized access to, acquisition of, and/or viewing of the PII of

Plaintiff and Class members by unauthorized third parties is highly offensive to a reasonable person.

82. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendant as part of obtaining services from Defendant, but privately and with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

83. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

84. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

85. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

86. As a proximate result of the above acts and omissions of Defendant, the

PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

87. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendant can be accessed, acquired, and viewed by unauthorized persons for years to come.

88. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff or Class members.

Third Claim – Breach of Implied Contract

89. Plaintiff incorporates by reference the allegations in paragraphs 11-47 above as though fully set forth herein.

90. When Plaintiff and Class members provided their PII to Defendant in connection with seeking wireless voice, messaging, and data services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' PII.

91. Defendant required Plaintiff and Class members to provide PII to receive wireless voice, messaging, and/or data services.

92. Defendant affirmatively represented that it collected and stored the PII of Plaintiff and Class members in using reasonable, industry standard means.

93. Based on Defendant's representations (as described above) and the implicit understanding of the parties, Plaintiff and Class members accepted Defendant's offers and provided Defendant with their PII.

94. Plaintiff and Class members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised.

95. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

96. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII.

97. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included (i) representing that it would maintain adequate data privacy and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections of Defendant's information systems; and (iii) failing to disclose to Plaintiff and Class members at the time they provided their PII that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

98. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (g) the diminished value of Plaintiff's and Class members' PII; (h) the diminished value of T-Mobile's services Plaintiff and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiff's and Class members' PII on the dark web.

Fourth Claim – Breach of Confidence

99. Plaintiff incorporates by reference the allegations in paragraphs 11-47

above as though fully set forth herein.

100. At all relevant times, Defendant was fully aware of the confidential nature of Plaintiff's and Class members' PII.

101. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by promises and expectations that Plaintiff and Class members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties.

102. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect the PII and not permit the PII to be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties.

103. Plaintiff and Class members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect their PII, such as following basic principles of protecting their networks and data systems.

104. Defendant voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the PII would not be accessed by, acquired by, disclosed to, or viewed by the public or any unauthorized third parties.

105. Due to Defendant's failure to prevent, detect, and avoid the Data Breach

from occurring by, *inter alia*, not following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was accessed by, acquired by, disclosed to, or viewed by unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

106. But for Defendant's failure to maintain and protect Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, disclosed to, or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiff's and Class members' PII, as well as the resulting damages.

107. As a direct and proximate result of Defendant's actions and omissions, Plaintiff and Class members have suffered damages as alleged herein.

108. The injury and harm Plaintiff and Class members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff's and Class members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiff's and Class members' PII had security and other vulnerabilities that placed Plaintiff's and Class members' PII in jeopardy.

109. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication,

and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (g) the diminished value of Plaintiff's and Class members' PII; (h) the diminished value of T-Mobile's services Plaintiff and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiff's and Class members' PII on the dark web.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned

as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

B. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment consumer data by, among other

things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks; and

vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

D. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

E. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

F. An award of such other and further relief as this Court may deem just

and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

****

DATED: August 19, 2021

HERMAN JONES LLP

By: /s/ *Peter M. Jones*

John C. Herman
(Ga. Bar No. 348370)
Peter M. Jones
(Ga. Bar No. 402620)
Carlton Jones
(Ga. Bar No. 940540)
3424 Peachtree Road, N.E., Suite 1650
Atlanta, Georgia 30326
Telephone: (404) 504-6500
Facsimile: (404) 504-6501
jherman@hermanjones.com
pjones@hermanjones.com
cjones@hermanjones.com

Counsel for Plaintiff